DETAILED ACTION

Response to Amendment

Status of the instant application:

- Claims 1 – 13, 18 – 20, 30 – 38, 43, 44 are pending in the instant application.
- Claims 14 - 17, 21 - 29, 39 - 42 are cancelled in the instant application.

Response to Arguments

Referring to claims 1 – 14, 16 – 20, 24 – 26, 28 – 44 that is under the 35 U.S.C. 103a rejection, that is obvious over Thomsen (US Patent NO. 7194004) in view of Renda et al. (US Patent No. 7127524), applicants amendment to the claims for examiners amendment and the remarks with the pre-appeal filed 02/25/2009 have been fully considered and have been found to be persuasive, therefore the rejection is withdrawn.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Karl T. Rees on 05/18/2009.

******Begin Examiners amendment to the claims************

Please replace claim 18 with this amended Claim 18:

18. A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

determining a user identifier associated with the network device that has caused a security event in the network;

in response to the security event, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;

wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;

wherein the second subset of addresses is different from the first subset of addresses; and

configuring one or more security restrictions with respect to the second network -- address.

Please replace claim 19 with this amended Claim 19:

19. An apparatus, comprising:

in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

means for determining a user identifier associated with the network device that has caused a security event in the network;

means for, in response to the security event, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;

wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;

wherein the second subset of addresses is different from the first subset of addresses; and

means for configuring one or more security restrictions with respect to the second network address.

Please replace claim 20 with this amended Claim 20:

20. An apparatus, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

in a security controller that is coupled, through the data network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

determining a user identifier associated with the network device that has caused a security event in the network;

in response to the security event, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;

wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;

wherein the second subset of addresses is different from the first subset of addresses; and

configuring one or more security restrictions with respect to the second network address.

Please replace claim 44 with this amended Claim 44:

44. A method, comprising the computer-implemented steps of:

in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

in response to a security event in the network, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;

wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;wherein causing the network device to acquire a second network address comprises performing an action that causes the network device to request a new network address;

Deleted: ¶

wherein the second subset of addresses is different from the first subset of addresses; and configuring one or more security restrictions with respect to the new network address.

*****End Examiners amendment to the claims******

Allowable Subject Matter

2. Claim(s) 1 – 13, 18 – 20, 30 – 38, 43, 44 allowed, but are renumbered as 1 – 27. The following is an examiner's statement of reasons for allowance: Applicants arguments that were filed with the pre - appeal on 02/25/2009 were found to be persuasive.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANT B. SHAIFER HARRIMAN whose telephone number is (571)272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

05/21/2009

/Dant B Shaifer - Harriman /
Examiner, Art Unit 2434

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434